A Generalized Wiener Attack on RSA

Johannes Blömer, Alexander May

Faculty of Computer Science, Electrical Engineering and Mathematics
University of Paderborn
33102 Paderborn, Germany
{*bloemer,alexx*}*@uni-paderborn.de*

Abstract. We present an extension of Wiener's attack on small RSA secret decryption exponents [10]. Wiener showed that every RSA public key tuple (N, e) with $e \in \mathbb{Z}^*_{\phi(N)}$ that satisfies $ed - 1 = 0 \bmod \phi(N)$ for some $d < \frac{1}{3}N^{\frac{1}{4}}$ yields the factorization of $N = pq$. Our new method finds p and q in polynomial time for every (N, e) satisfying $ex + y = 0 \bmod \phi(N)$ with

$$x < \frac{1}{3}N^{\frac{1}{4}} \quad \text{and} \quad |y| = \mathcal{O}(N^{-\frac{3}{4}}ex).$$

In other words, the generalization works for all secret keys $d = -xy^{-1}$, where x, y are suitably small. We show that the number of these weak keys is at least $N^{\frac{3}{4}-\epsilon}$ and that the number increases with decreasing prime difference $p - q$. As an application of our new attack, we present the cryptanalysis of an RSA-type scheme presented by Yen, Kim, Lim and Moon [11, 12]. Our results point out again the warning for crypto-designers to be careful when using the RSA key generation process with special parameters.

Keywords: RSA, weak keys, Wiener attack, continued fractions

1 Introduction

Let $N = pq$ be an RSA-modulus, where p and q are primes of equal bit-size (wlog $p > q$). Let e be the public exponent and d be the secret exponent satisfying $ed = 1 \bmod \phi(N)$, where $\phi(N)$ is the Euler totient function. We denote by $\mathbb{Z}^*_{\phi(N)}$ the multiplicative group of invertible integers modulo $\phi(N)$. An RSA public key is a tuple $(N, e) \in \mathbb{Z} \times \mathbb{Z}^*_{\phi(N)}$.

In order to study the security of RSA, many people focus on the difficulty to factor the modulus N without taking into account additional information that may be encoded in the public exponent e. Hence, it is tempting for crypto-designers to construct RSA-type schemes with special public exponents that yield a good performance in encryption/decryption. For example, one might be tempted to use small decryption exponents d in order to speed up the decryption process. Another fast RSA-variant that makes use of special RSA-keys was proposed by Yen, Kim, Lim and Moon [11, 12] in 2001. This YKLM-scheme is designed to counteract the fault-based attack on CRT-RSA of Boneh, DeMillo and Lipton [2].

In 1990, Wiener [10] observed that information encoded in the public exponent e might help to factor N. More precisely, he showed that every public exponent $e \in \mathbb{Z}^*_{\phi(N)}$ that corresponds to a secret exponent d with $d \leq \frac{1}{3}N^{\frac{1}{4}}$ yields the factorization of the modulus in time polynomial in $\log(N)$. In 1999, Boneh and Durfee [3] used Coppersmith's method for finding small roots of modular polynomial equations [4] to improve the bound to $d \leq N^{0.292}$.

Although the YKLM-scheme uses a special key generation algorithm in order to provide good performance, the secret keys d are not chosen to be small. Therefore, the Wiener attack as well as the Boneh-Durfee attack cannot directly be applied to this RSA-variant. However, in this work we present an extension of Wiener's approach that leeds to a much larger class of secret keys d which are insecure. Furthermore, we show that the keys which are generated in the YKLM-scheme belong to this larger class, for all reasonable parameter choices of the scheme. As a result, we obtain that the public keys (N, e) in the YKLM-scheme yield the factorization of N in polynomial time.

Let us put the cryptanalytic approaches above into a more general framework by defining the notion of *weak keys*: The results so far show that there are classes of public keys (N, e) where every element in the class yields the factorization of N. One may view the auxiliary input e as a hint how to factor N: Without having e we assume that factoring N is hard, but with the help of e it becomes feasible. In the case of the Wiener attack the class consists of all public key tuples (N, e) where $ed - 1 = 0 \bmod \phi(N)$ with $d < \frac{1}{3}N^{\frac{1}{4}}$.

We call such a class *weak* and the elements (N, e) of the weak class are called *weak keys*. To be more precisely: We define the size of a class of public key tuples by the number of elements (N, e) in the class for every fixed N. Let C be a class of public key tuples (N, e), then

$$\text{size}_C(N) = |\{e \in \mathbb{Z}^*_{\phi(N)} \mid (N, e) \in C\}|.$$

C is called *weak* if

1. The size of C is polynomial in N, i.e. $\text{size}_C(N) = \Omega(N^\gamma)$ for some $\gamma > 0$.
2. There exists a probabilistic algorithm A that on every input $(N, e) \in C$ outputs the factorization of N in time polynomial in $\log(N)$.

Note that the size of a weak class is a function in N which denotes the number of elements that can be factored by the corresponding algorithm A. For example, the size of the class in the Wiener attack is at least $N^{\frac{1}{4}-\epsilon}$. Here the ϵ-term comes from the fact that only those d with $\gcd(d, \phi(N)) = 1$ define legitimate RSA-keys.

Let us give another (trivial) example of a weak class of public keys. Every tuple (N, e) with $e = kq$, $1 < k < p$ is a weak key, since the computation $\gcd(N, e) = q$ yields the factorization. These are $p > N^{\frac{1}{2}}$ many weak keys. Howgrave-Graham [6] observed that even the knowledge of $e = kq + r$ for some unknown $r \leq N^{\frac{1}{4}}$ suffices to find the factorization of N. This implies the existence of a weak class with size $N^{\frac{3}{4}}$.

We think that it is a very natural question to study how many of the possible choices of the public keys are indeed weak keys that should not be used in the design of crypto-systems. For the Wiener attack and the Boneh-Durfee attack it is easy for a crypto-designer to see that a key is weak by inspecting the most significant bits of d. For the extension of Wiener's attack that we describe in this paper the weakness of the keys is not obvious. One can understand our new result as a warning for crypto-designers to be careful when using keys with a special structure.

There is also an imminent danger from weak keys in the case of untrusted servers that create public/secret key pairs: Crépeau and Slakmon [5] showed how to use weak keys in order to construct malicious RSA systems by encoding information into the public exponent e. Our new class of weak keys is well-suited for the use in such systems and leads to a large variety of new malicious keys.

In order to describe our new attack, let us first consider the normal RSA-case, where $p - q = \Omega(\sqrt{N})$. Note that for randomly chosen primes of the same bitsize, the probability that p, q agree in the c most significant bits is roughly $2^{-(c-1)}$. Hence, we have $p - q = \Omega(\sqrt{N})$ with overwhelming probability.

For the case $p - q = \Omega(\sqrt{N})$, we introduce a variant of Wiener's attack that works for all public keys (N, e) where $ex + y = k\phi(N)$, $k \in \mathbb{N}$ with

$$0 < x \leq \frac{1}{3} N^{\frac{1}{4}} \quad \text{and} \quad |y| = \mathcal{O}(N^{-\frac{3}{4}} ex).$$

Notice that our bounds exclude trivial solutions where $ex + y = 0$, since $|y| < ex$.

The new method works as follows: As in Wiener's approach, we use the continued fraction algorithm to recover the unknown values x and k. Afterwards, we show that a factorization method due to Coppersmith [4] can be applied: Given half of the most significant bits of p, one can find the factorization of N.

Let us compare the new result to Wiener's attack. Our weak keys have the structure that $e^{-1} = d = -\frac{x}{y} \bmod \phi(N)$, i.e. Wiener's algorithm is the special case where $x = d$ and $y = -1$. One should observe that for x of size roughly $N^{\frac{1}{4}}$ as in Wiener's attack, the parameter e must be of size at least $N^{\frac{3}{4}}$ in order to satisfy a relation of the form $ex + y = 0 \bmod \phi(N)$. Thus, $|y|$ can be chosen of size at least x. If e is roughly N, which is normally the case for small d, $|y|$ can even be chosen of size $N^{\frac{1}{4}} x$ in the attack.

One should expect that for fixed N the number of public keys (N, e) for which our approach applies is roughly the number of tuples (x, y) within the given bounds. This number can be upper bounded by $x \cdot N^{\frac{1}{4}} x \leq N^{\frac{3}{4}}$. In fact, we are able to show that the number of weak keys (N, e) for which our algorithm works is also lower bounded by $\Omega(N^{\frac{3}{4} - \epsilon})$.

It is important to notice that in contrast to the approaches of Wiener and Boneh-Durfee, the secret keys in our attack are not small itself but have a "small decomposition" in x and y. So they might look innocuous to crypto-designers and may be tempting to use in the design of cryto-systems with good encryption/decryption performance.

As an example, we show that the public keys (N, e) constructed in the YKLM-scheme can be attacked by our generalization of Wiener's method. Namely, we can express the secret exponent d in terms of small x and y, which breaks the crypto-system for all reasonable parameter choices.

In 2002, de Weger [9] observed that Wiener's attack can be improved when the prime difference $p-q$ is significantly less than $\sqrt{N}$. de Weger's method also applies to our extension of Wiener's attack. Interestingly, we are able to show that for prime difference $p-q = N^{\frac{1}{4}+\gamma}$, $0 < \gamma \leq \frac{1}{4}$ there are at least $N^{1-\gamma-\epsilon}$ weak RSA-keys (N, e).

It is important to notice that for prime difference $p-q = \mathcal{O}(N^{\frac{1}{4}})$ an algorithm of Fermat finds the factorization in polynomial time. Thus, our attack has a nice interpolation property towards Fermat's algorithm: As $p-q$ decreases, the number of weak public keys increases. For γ approaching zero almost all keys are weak, corresponding to the fact that N can be easily factored without any hint that is encoded in e.

As a by-product, we get a simple probabilistic factorization algorithm with expected running time $\mathcal{O}(N^{\gamma+\epsilon})$ comparable to Fermat-Factorization: For a fixed N, choose random $e < N$ and apply our algorithm to each choice (N, e) until (N, e) is a weak key that yields the factorization.

Notice that the interpolation property above seems to imply that one cannot improve our approach significantly. On the other hand, there might be different techniques – for example lattice reduction techniques for higher dimensional lattices – that lead to larger classes of weak keys for the prime difference $p-q = \Omega(\sqrt{N})$. But at the moment this is an open question.

The paper is organized as follows: In Section 2, we present our extension of Wiener's attack. As an application of this method, we present the crytanalysis of the YKLM-scheme in Section 3. In Section 4, we apply the methods of de Weger to our generalized Wiener attack. We conclude the paper by showing in Section 5 that the number of weak RSA-keys (N, e) in our approach is $\Omega(N^{\frac{3}{4}-\epsilon})$.

2 The generalized Wiener attack

Throughout this work we consider RSA-moduli $N = pq$, where p and q are of the same bit-size (wlog $p > q$). This implies the inequalities

$$p - q \leq N^{\frac{1}{2}} \quad \text{and} \quad 2N^{\frac{1}{2}} \leq p + q \leq 3N^{\frac{1}{2}}.$$

Furthermore, we have $\phi(N) = N + 1 - (p + q) > \frac{N}{2}$.
Our attack makes use of a well-known result due to Coppersmith [4]:

Theorem 1 (Coppersmith) *Let $N = pq$ be an RSA-modulus, where p and q are of the same bit-size. Suppose we are given an approximation of p with additive error at most $N^{\frac{1}{4}}$. Then N can be factored in time polynomial in* $\log N$.

We are now able to state our main theorem. Here we consider the normal RSA-case where $p - q = \Omega(\sqrt{N})$.

Theorem 2 *Let $c \leq 1$ and let (N, e) be an RSA public key tuple with $N = pq$ and $p - q \geq cN^{\frac{1}{2}}$. Suppose that $e \in Z^*_{\phi(N)}$ satisfies an equation $ex + y = k\phi(N)$ with*

$$0 < x \leq \frac{1}{3}N^{\frac{1}{4}} \quad \text{and} \quad |y| \leq cN^{-\frac{3}{4}}ex.$$

Then N can be factored in polynomial time.

One should notice that the conditions of Theorem 2 imply that $ex + y \neq 0$, thereby excluding trivial congruences: Since $c \leq 1$, we see that $|y| < ex$. This in turn implies $k > 0$.

Roadmap for the Proof of Theorem 2

- We show that the unknown parameters x, k can be found among the convergents of the continued fraction expansion of $\frac{e}{N}$.
- From x and k, we compute an approximation of $p + q$.
- From an approximation of $p + q$, we compute an approximation of $p - q$.
- Combining both approximations gives us an approximation of p, which leads to the factorization of N by using Coppersmith's Theorem.

We want to argue that in the following proof we can assume wlog that $N \geq (\frac{8}{c})^4$. This condition is equivalent to $c \geq 8N^{-\frac{1}{4}}$. If this inequality does not hold then $p - q = \mathcal{O}(N^{\frac{1}{4}})$ and Fermat's factorization algorithm yields the factorization of N in polynomial time.

Proof: Let us start with the RSA key equation

$$ex + y = k(N - p - q + 1). \tag{1}$$

Dividing by Nx gives us

$$\frac{e}{N} - \frac{k}{x} = -\frac{k(p + q - 1) + y}{Nx}.$$

We want to argue that we can assume wlog that $\gcd(k, x) = 1$. Notice that every integer that divides both k and x must also divide y by equation (1). Thus, we can divide equation (1) by $\gcd(k, x)$ which gives us an equation $ex' + y' = 0 \bmod \phi(N)$ with even smaller parameters x' and y'. Hence we can assume that $\frac{k}{x}$ is a fraction in its lowest terms.

By a well-known theorem (see e.g. Theorem 184 in [7]), the fraction $\frac{k}{x}$ appears among the convergents of $\frac{e}{N}$ if the condition $|\frac{e}{N} - \frac{k}{x}| < \frac{1}{2x^2}$ is satisfied. Thus it remains to show that $|k(p + q - 1) + y| < \frac{N}{2x}$. Let us first find a bound for the parameter k. We know that $k = \frac{ex+y}{\phi(N)}$ and $|y| \leq cN^{-\frac{3}{4}}ex$. Since our precondition $N \geq (\frac{8}{c})^4$ implies $N \geq 2^{12}$, we conclude that $|y| \leq \frac{1}{4}ex$. Therefore, we obtain

$$\frac{3}{4}\frac{ex}{\phi(N)} \leq k \leq \frac{5}{4}\frac{ex}{\phi(N)}. \tag{2}$$

Now we are able to estimate

$$k(p+q-1)+y \leq \frac{15}{4}\frac{ex}{\phi(N)} \cdot N^{\frac{1}{2}} + cN^{-\frac{3}{4}}ex \leq \frac{15}{4}xN^{\frac{1}{2}} + xN^{\frac{1}{4}} \leq 4xN^{\frac{1}{2}},$$

where the last inequality holds for $N \geq 2^{12}$.

Therefore, we have to satisfy the condition $4xN^{\frac{1}{2}} < \frac{N}{2x}$ which is equivalent to $x < \frac{1}{\sqrt{8}}N^{\frac{1}{4}}$. This condition holds by our upper bound $x \leq \frac{1}{3}N^{\frac{1}{4}}$.

Hence, the fraction $\frac{k}{x}$ must be among the convergents of the continued fraction expansion of $\frac{e}{N}$. Since there are only $\mathcal{O}(\log N)$ many convergents, we can apply the following process to each candidate for k and x until our algorithm succeeds.

We have to show that the correct k and x yield the factorization of N. Let us write equation (1) as

$$N+1-\frac{ex}{k} = p+q+\frac{y}{k}.$$

Since every parameter on the left hand side is now known to us, we can compute an approximation of $p+q$ up to some unknown error term $\frac{y}{k}$, that can be bounded by $|\frac{y}{k}| \leq \frac{4}{3}cN^{\frac{1}{4}}$ using inequality (2).

Our goal is to find an approximation of p up to some error of size $N^{\frac{1}{4}}$ in order to apply Coppersmith's theorem. Therefore, we transform our approximation of $p+q$ into an approximation of $p-q$ using the relation

$$p-q = \sqrt{(p-q)^2} = \sqrt{(p+q)^2-4N}.$$

Let s be our approximation of $p+q$ with additive error at most $\frac{4}{3}cN^{\frac{1}{4}}$. We will show that $t = \sqrt{s^2-4N}$ is an approximation of $p-q$ with an additive error that can be bounded by $9N^{\frac{1}{4}}$. Thus, the term $\frac{1}{2}(s+t)$ is an approximation of p with error at most

$$\begin{aligned}
\left|\frac{1}{2}(s+t)-p\right| &= \frac{1}{2}|s-p-q+t-p+q| \\
&\leq \frac{1}{2}\left|s-(p+q)\right| + \frac{1}{2}\left|t-(p-q)\right| \\
&\leq \frac{2}{3}cN^{\frac{1}{4}} + \frac{9}{2}N^{\frac{1}{4}} \leq 6N^{\frac{1}{4}}
\end{aligned}$$

Define $\tilde{p} = \frac{1}{2}(s+t)$. Then one out of the six values $\tilde{p}+(2k+1)N^{\frac{1}{4}}$, $k = -3,-2,-1,0,1,2$ is an approximation of p up to an error of at most $N^{\frac{1}{4}}$ in absolute value. We can apply Coppersmith's algorithm to all these values. The correct term will then lead to the factorization of N in polynomial time.

It remains to show that $t = \sqrt{s^2-4N}$ is indeed an approximation of $p-q$ up to some error term that can be bounded by $9N^{\frac{1}{4}}$. Let us first show that t is well-defined, i.e. $s^2-4N \geq 0$. Observe that $s = p+q+\frac{y}{k}$ satisfies

$$s^2-4N = (p-q)^2 + 2\frac{y}{k}(p+q) + \left(\frac{y}{k}\right)^2.$$

Therefore, it suffices to show that $|2\frac{y}{k}(p+q)| \leq (p-q)^2$. Using $|\frac{y}{k}| \leq \frac{4}{3}cN^{\frac{1}{4}}$, we obtain $|2\frac{y}{k}(p+q)| \leq 8cN^{\frac{3}{4}}$. From our precondition $N \geq (\frac{8}{c})^4$, we see that $8 \leq cN^{\frac{1}{4}}$. This immediately implies $8cN^{\frac{3}{4}} \leq c^2N \leq (p-q)^2$ as desired.

Since $N \geq 2^{12}$, we know that the error term $\frac{y}{k}$ for $p+q$ can be bounded in absolute value by $\frac{4}{3}cN^{\frac{1}{4}} \leq \frac{1}{2}N^{\frac{1}{2}} \leq \frac{1}{4}(p+q)$. This implies the inequality

$$s \leq \frac{5}{4}(p+q). \tag{3}$$

We observe that

$$t-(p-q) = \sqrt{s^2-4N}-(p-q) = \frac{(s-(p+q))(s+(p+q))}{\sqrt{s^2-4N}+(p-q)}.$$

Using the inequalities (3), $s-(p+q) \leq \frac{4}{3}cN^{\frac{1}{4}}$ and $p-q \geq cN^{\frac{1}{2}}$ finally leads us to the desired bound

$$t-(p-q) \leq \frac{\frac{4}{3}cN^{\frac{1}{4}} \cdot \frac{27}{4}N^{\frac{1}{2}}}{(p-q)} \leq 9N^{\frac{1}{4}}.$$

Let us briefly summarize the whole factorization algorithm.

Algorithm Generalized Wiener Attack

INPUT: (N,e), where $N=pq$ and $ex+y=0 \bmod \phi(N)$ for some unknown $0<x\leq \frac{1}{3}N^{\frac{1}{4}}$ and $|y| \leq cN^{-\frac{3}{4}}ex$.

1. Compute the continued fraction expansion of $\frac{e}{N}$.
2. For every convergent $\frac{k}{x}$ of the expansion:
   (a) Compute $s = N+1-\frac{ex}{k}$, $t=\sqrt{s^2-4N}$ and $\tilde{p}=\frac{1}{2}(s+t)$.
   (b) Apply Coppersmith's algorithm to the candidates $\tilde{p}+(2k+1)N^{\frac{1}{4}}$ for $k=-3,-2,\ldots,2$: If Coppersmith's algorithm outputs the factorization of N, then stop.

OUTPUT: p,q

Since every step in Algorithm Generalized Wiener-Attack can be done in polynomial time and the number of convergents is bounded by $\mathcal{O}(\log N)$, this concludes the proof of Theorem 2. $\square$

3 Cryptanalysis of the YKLM-scheme

In 2001, Yen, Kim, Lim and Moon [11, 12] presented an RSA-type scheme that was designed to counteract the Bellcore-attack (see [2]). Unfortunately, they need a specialized RSA key generation process in order to make their scheme efficient. Their public key e satisfies a relation with some small parameters that will be described in this section. The efficiency of the YKLM-scheme relies on the fact that these parameters are indeed much smaller than the modulus N. It was raised as an open question by the authors if one can use random public keys e as well in their scheme, thereby maintaining the same performance.

We show that the public keys constructed in the YKLM-scheme satisfy the conditions of Theorem 2, i.e. for every public exponent e we have $ex + y = 0 \bmod \phi(N)$ with small x and y.

Let us first reconsider the modified key generation algorithm in the YKLM-scheme.

RSA Key Generation in the YKLM-scheme

Modulus : Choose randomly two primes p and q of the same bit-size and compute the product $N = pq$.

Small parameters : Fix a bound B, where $B \ll N$. Choose randomly e_r and r in $\{1, \dots, B\}$ such that $\gcd(e_r, \phi(N)) = 1$. Compute $d_r = e_r^{-1} \bmod \phi(N)$.

Secret exponent : Compute $d = d_r + r$. If $\gcd(d, \phi(N)) \neq 1$, choose different parameters e_r and r.

Public exponent : Compute $e = d^{-1} \bmod \phi(N)$.

Public parameters : Publish the tuple (N, e).

The authors pointed out that instead of the public key tuple (N, e) one could even publish the parameters e_r and r as well, but the following observation shows that the parameters e_r and r immediately yield the factorization of N.

Consider the public key equation

$$ed - 1 = 0 \bmod \phi(N)$$

The secret key d has a decomposition into the unknown part d_r and the known parameter r

$$e(d_r + r) - 1 = 0 \bmod \phi(N).$$

Multiplication with e_r removes the unknown parameter d_r

$$e(1 + e_r r) - e_r = 0 \bmod \phi(N).$$

Since every parameter on the left hand side is known, we can compute a multiple $k\phi(N)$ of the Euler function

$$e(1 + e_r r) - e_r = k\phi(N) \quad \text{for some } k \in \mathbb{N}. \tag{4}$$

Since $e < \phi(N)$, we have that $k < (1 + e_r r)$. Therefore, the bit-length of k is polynomial in the bit-length of N. It is a well-known result that such a multiple $k\phi(N)$ yields the factorization of N in probabilistic polynomial time in the bit-length of N (see for example [8]).

Certainly, there is no need to publish the small parameters e_r and r in the YKLM-scheme. On the other hand, we see that by equation (4) one can apply Theorem 2 by setting $x = 1 + e_r r$ and $y = -e_r$. This gives us the following corollary from Theorem 2.

Corollary 3 *Let $c \leq 1$ and let (N, e) be a public key tuple constructed by the key generation process in the YKLM-scheme with $p - q \geq cN^{\frac{1}{2}}$. Furthermore, let e_r and r satisfy the conditions*

$$1 + e_r r \leq \frac{1}{3}N^{\frac{1}{4}} \quad \text{and} \quad e_r \leq \frac{1}{2}cN^{\frac{1}{4}}$$

Then N can be factored in time polynomial in $\log(N)$.

Proof: In order to be able to apply Theorem 2, it remains to show that $\frac{1}{2}cN^{\frac{1}{4}} \leq cN^{-\frac{3}{4}}e(1 + e_r r)$. Using equation (4), we conclude that

$$cN^{-\frac{3}{4}}e(1 + e_r r) > cN^{-\frac{3}{4}}\phi(N) > \frac{1}{2}cN^{\frac{1}{4}},$$

which proves the claim. ⊒

Since the efficiency of the YKLM-scheme relies on the fact that e_r and r are very small compared to N, Corollary 3 breaks the YKLM-scheme for all reasonable parameter choices.

4 Generalizing to arbitrary prime differences $p - q$

de Weger [10] observed that Wiener's attack can be improved when $p - q$ is significantly smaller than $\sqrt{N}$. He showed that $N' = N - \lfloor 2\sqrt{N} \rfloor$ is an approximation of $\phi(N)$ with error at most $\frac{(p-q)^2}{\sqrt{N}}$. Thus, using the continued fraction expansion $\frac{e}{N'}$ instead of $\frac{e}{N}$ leads to an improvement in Wiener's algorithm. Namely, de Weger proved that for prime differences $p - q$ of size $N^{\frac{1}{4}+\gamma}$, $0 \leq \gamma \leq \frac{1}{4}$ one can achieve a bound of $d \leq N^{\frac{1}{2}-\gamma}$ in Wiener's algorithm.

The same trick applies to our generalized version of Wiener's attack (Section 2) as well. This gives us the following more general result.

Theorem 4 *Given an RSA public key tuple (N, e), where $N = pq$. Suppose that e satisfies an equation $ex + y = 0 \bmod \phi(N)$ with*

$$0 < x \leq \frac{1}{3}\sqrt{\frac{\phi(N)}{e}}\frac{N^{\frac{3}{4}}}{p - q} \quad \text{and} \quad |y| \leq \frac{p - q}{\phi(N)N^{\frac{1}{4}}} \cdot ex.$$

Then N can be factored in time polynomial in $\log N$.

Proof. The proof is similar to the proof of Theorem 2. One mainly substitutes N by $N' = N - \lfloor 2\sqrt{N} \rfloor$ and works through the arithmetic. Therefore we omit the proof.

Instead we give the factorization algorithm.

Algorithm Generalized Wiener Attack II

INPUT: (N, e), where $N = pq$ and $ex + y = 0 \bmod \phi(N)$ for some unknown $0 < x \leq \frac{1}{3}\sqrt{\frac{\phi(N)}{e}\frac{N^{\frac{3}{4}}}{p-q}}$ and $|y| \leq \frac{p-q}{\phi(N)N^{\frac{1}{4}}} \cdot ex$.

1. Set $N' = N - \lfloor 2\sqrt{N} \rfloor$ and compute the continued fraction expansion of $\frac{e}{N'}$.
2. For every convergent $\frac{k}{x}$ of the expansion:
   (a) Compute $s = N + 1 - \frac{ex}{k}$, $t = \sqrt{s^2 - 4N}$ and $\tilde{p} = \frac{1}{2}(s + t)$.
   (b) Apply Coppersmith's algorithm to the candidates $\tilde{p} + (2k + 1)N^{\frac{1}{4}}$ for $k = -3, -2, \ldots, 2$: If Coppersmith's algorithm outputs the factorization of N, then stop.

OUTPUT: p, q

5 There Are $N^{\frac{3}{4}-\epsilon}$ Weak RSA-Keys

In Section 4, we showed that every public key tuple (N, e) that satisfies a relation $ex + y = 0 \bmod \phi(N)$, with

$$0 < x \leq \frac{1}{3}\sqrt{\frac{\phi(N)}{e}\frac{N^{\frac{3}{4}}}{p-q}} \quad \text{and} \quad |y| \leq \frac{p-q}{\phi(N)N^{\frac{1}{4}}} \cdot ex. \tag{5}$$

yields the factorization of N in polynomial time. Those tuples (N, e) are *weak keys* that should not be used in the design of a crypto-system. Let us formalize the notion of weak keys.

Definition 5 *Let C be a class of RSA public keys (N, e). The size of the class C is defined by*

$$size_C(N) = |\{e \in \mathbb{Z}^*_{\phi(N)} \mid (N, e) \in C\}|.$$

C is called weak *if:*

1. *$size_C(N) = \Omega(N^\gamma)$ for some $\gamma > 0$.*
2. *There exists a probabilistic algorithm A that on every input $(N, e) \in C$ outputs the factorization of N in time polynomial in $\log(N)$.*

The elements of a weak class are called weak keys*.*

Our variant of Wiener's attack in Section 4 defines a weak class C. The question we will study in this chapter is, how large this weak class is.

What bounds can we expect for $\text{size}_C(N)$? As a first estimate we can sum over all tuples (x, y) within the bounds given by the inequalities in (5). This gives us an upper bound on the size of C. Therefore, we have at most

$$\text{size}_C(N) \leq \left(\frac{1}{3}\sqrt{\frac{\phi(N)}{e}\frac{N^{\frac{3}{4}}}{p-q}}\right)^2 \cdot \frac{e}{\phi(N)}\frac{p-q}{N^{\frac{1}{4}}} = \mathcal{O}\left(\frac{N^{\frac{5}{4}}}{p-q}\right) \tag{6}$$

weak keys. This is an upper bound on $\text{size}_C(N)$ since:

- Different tuples (x, y) might define the same public exponent e.
- Some of the tuples (x, y) do not even define a legitimate public key e, e.g. a key $e \in Z^*_{\phi(N)}$.

Instead of an upper bound on $\text{size}_C(N)$, we are interested in a lower bound. Namely, we want to know the minimal number of public exponents $e \in \mathbb{Z}^*_{\phi(N)}$ that yield the factorization for some fixed modulus N. In this section we will prove a lower bound for $\text{size}_C(N)$.

As the result we obtain that our lower bound almost perfectly matches the upper bound: If $p - q = \Omega(N^{\frac{1}{4}+\gamma})$, $\gamma > 0$, we obtain a lower bound of

$$\text{size}_C(N) = \Omega\left(\frac{N^{\frac{5}{4}-\epsilon}}{p-q}\right).$$

Let us have a closer look at this result. In the common RSA case, we have $p - q = \mathcal{O}(N^{\frac{1}{2}})$ which implies a bound of

$$\text{size}_C(N) = \Omega\left(N^{\frac{3}{4}-\epsilon}\right)$$

weak RSA key tuples (N, e).

On the other hand, we know that Fermat's factorization algorithm yields the factorization of N in polynomial time if $p - q = \mathcal{O}(N^{\frac{1}{4}})$. But the number of weak keys for $p - q = N^{\frac{1}{4}+\gamma}$, $0 < \gamma \leq \frac{1}{4}$ is $\Omega(N^{1-\gamma-\epsilon})$. That means that the number of weak keys scales almost perfectly with the prime difference $p - q$. As $p - q$ decreases, the number of weak key tuples increases and as γ approaches zero almost all keys are weak. This corresponds to the fact that for $\gamma = 0$, all tuples (N, e) are weak because one can find the factorization of N in polynomial time with Fermat's algorithm.

We will now prove the lower bound result, where we use the following main lemma.

Lemma 6 *Let $f(N, e)$, $g(N, e)$ be functions such that $f^2(N, e)g(N, e) < \phi(N)$, $f(N, e) \geq 2$ and $g(N, e) \leq f(N, e)$. The number of public keys $e \in \mathbb{Z}^*_{\phi(N)}$, $e \geq \frac{\phi(N)}{4}$ that satisfy an equation $ex + y = 0 \bmod \phi(N)$ for $x \leq f(N, e)$ and $|y| \leq g(N, e)x$ is at least*

$$\frac{f^2(N, e)g(N, e)}{8 \log\log^2(N^2)} - \mathcal{O}(f^2(N, e)N^{\epsilon}),$$

where $\epsilon > 0$ is arbitrarily small for N suitably large.

Using Lemma 6, we can immediately prove our lower bound theorem.

Theorem 7 *Let* $p - q = N^{\frac{1}{4}+\gamma}$ *with* $0 < \gamma \leq \frac{1}{4}$*. Further, let* C *be the weak class that is given by the public key tuples* (N, e) *defined in Theorem 4 with the additional restriction that* $e \in Z^*_{\phi(N)}$*,* $e \geq \frac{\phi(N)}{4}$*. Then*

$$size_C(N) = \Omega\left(\frac{N^{1-\gamma}}{\log\log^2(N^2)}\right).$$

Proof: Using the bounds of (5), we define

$$f(N,e) = \frac{1}{3}\sqrt{\frac{\phi(N)}{e}}\frac{N^{\frac{3}{4}}}{p-q} \quad \text{and} \quad g(N,e) = \frac{e}{\phi(N)}\frac{p-q}{N^{\frac{1}{4}}}.$$

It can be easily checked that these settings fulfill the requirements of Lemma 6:

$$f^2(N,e)g(N,e) < \phi(N),\ f(N,e) \geq 2 \text{ and } g(N,e) \leq f(N,e).$$

Hence, we can apply Lemma 6. Since $g(N,e) = \Omega(N^\gamma)$, the term

$$\frac{f^2(N,e)g(N,e)}{8\log\log^2(N^2)}$$

dominates the error term $\mathcal{O}(f^2(N,e)N^\epsilon)$.
Using $f^2(N,e)g(N,e) = \Omega(\frac{N^{\frac{5}{4}}}{p-q})$ and $p - q = N^{\frac{1}{4}+\gamma}$ proves the claim. $\square$

We obtain the following corollary.

Corollary 8 *Let* C *be the weak class that is given by the public key tuples* (N, e) *defined in Theorem 2 with the additional restriction that* $e \in \mathbb{Z}^*_{\phi(N)}$*,* $e \geq \frac{\phi(N)}{4}$*. Then*

$$size_C(N) = \Omega\left(\frac{N^{\frac{3}{4}}}{\log\log^2(N^2)}\right).$$

It remains to prove Lemma 6. Since the proof is technical, we describe just the rough idea and leave the details to the appendix.

As denoted before, different tuples (x, y) might define the same public exponent e and some tuples (x, y) do not define a legitimate key $e \in Z^*_{\phi(N)}$. Therefore, we define a suitably large subclass T of all tuples (x, y) within the given bounds $x \leq f(N,e)$ and $|y| \leq g(N,e)x$ such that different tuples define different legitimate keys e.

The definition of the class T and the details of the proof can be found in the appendix.

References

1. T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, 1980.
2. D. Boneh, R. DeMillo, R. Lipton, "On the importance of checking cryptographic protocols for faults", in *Proceedings of Eurocrypt'97*, Lecture Notes in Computer Science, Vol. 1233, Springer Verlag, 1997.
3. D. Boneh, G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$", *IEEE Trans. on Information Theory*, Vol. 46(4), 2000
4. D. Coppersmith, "Small solutions to polynomial equations and low exponent vulnerabilities", *Journal of Cryptology*, Vol. 10(4), pp. 223–260, 1997.
5. C. Crépeau, A. Slakmon, "Simple Backdoors for RSA Key Generation", in *Topics in Cryptology - CT-RSA 2003*, Lecture Notes in Computer Science Vol. 2612, pp. 403–416, Springer-Verlag, 2003
6. N. Howgrave-Graham, "Approximate integer common divisors", *Cryptography and Lattices*, Lecture Notes in Computer Science, Vol. 2146, Springer-Verlag, 2001.
7. G. H. Hardy, E. M. Wright, *Introduction to the theory of numbers*, Oxford University Press, 1979.
8. N. Koblitz, *A course in number theory and cryptography*, Springer-Verlag, 1994
9. B. de Weger, "Cryptanalysis of RSA with small prime difference", *Applicable Algebra in Engineering, Communication and Computing*,Vol. 13(1), pp. 17–28, 2002.
10. M. Wiener, "Cryptanalysis of short RSA secret exponents", *IEEE Transactions on Information Theory*, Vol. 36, pp. 553–558, 1998.
11. S. -M. Yen, S. Kim, S. Lim, S. Moon, "Speedup with Residue Number System Immune against Hardware Fault Cryptanalysis", 4^{th} *International Conference on Information Security and Cryptology*, Lecture Notes in Computer Science, Vol. 2288, pp. 397–413, Springer-Verlag, 2001.
12. S. -M. Yen, S. Kim, S. Lim, S. Moon, "RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis", *IEEE Transactions on Computers*, Vol. 52(4), 2003

Appendix: Proof of Lemma 6

Throughout the following proof, we will use the shorthand notations f and g for $f(N, e)$ and $g(N, e)$, respectively. Let us recall the preconditions of Lemma 6: We consider public keys that satisfy a relation $ex + y = k\phi(N)$ for some $k \in \mathbb{N}$, where the parameters x and y satisfy the bounds $x \leq f$ and $|y| \leq gx$.

Roadmap for the proof of Lemma 6

We define a set T which is a union of pairwise disjoint subsets $T(k)$. Each subset $T(k)$ consists of tuples (x, y) – x, y within the given bounds – such that

- Every $(x, y) \in T(k)$ defines a public key $e \in \mathbb{Z}^*_{\phi(N)}$ with $ex + y = k\phi(N)$.
- Different $(x, y) \in T$ (not only in $T(k)$!) define different public keys e.
- $|T| \geq \frac{f^2 g}{8 \log \log^2(N^2)} - \mathcal{O}(f^2 N^{\epsilon})$

Let us define the sets $T(k)$ and their union T.

Definition 9 *For every fixed N and for every $k \in \mathbb{Z}$ define the set*

$$T(k) := \left\{ (x,y) \in \mathbb{N} \times \mathbb{Z} \,\middle|\, \begin{array}{c} k < x < f\,,\ |y| \le gx, y = k\phi(N) \bmod x, \\ \gcd(x, k\phi(N)) = 1, \gcd(y, \phi(N)) = 1 \end{array} \right\}.$$

Further define

$$T = \bigcup_{k=\frac{f}{4}+1}^{f} T(k).$$

The rest of the proof of Lemma 6 is dedicated to the verification of the three properties stated in the roadmap above.

The following lemma shows that each tuple $(x,y) \in T(k)$ defines a public exponent $e \in Z^*_{\phi(N)}$ of the desired form.

Lemma 10 *For every tuple $(x,y) \in T(k)$ there is an $e \in Z^*_{\phi(N)}$ such that $ex + y = k\phi(N)$.*

Proof: Since $y = k\phi(N) \bmod x$ by Definition 9, there exists an integer e such that $ex + y = k\phi(N)$.

Using $0 < k < x$ and $|y| \le gx < gf^2 < \phi(N)$, we obtain

$$0 < e = \frac{k\phi(N) - y}{x} \le \frac{k\phi(N) - y}{k+1} < \phi(N).$$

Finally since $\gcd(y, \phi(N))$, we have

$$\gcd(ex, \phi(N)) = \gcd(k\phi(N) - y, \phi(N)) = 1,$$

and therefore $\gcd(e, \phi(N)) = 1$ which concludes the proof. $\square$

Next we want to show that different tuples (x,y) lead to different public keys.

Lemma 11 *Let (x_0, y_0) and (x_1, y_1) be two different tuples from T. Then they define distinct public exponents.*

Proof: According to Lemma 10, there exist $e_0, e_1 \in \mathbb{Z}^*_{\phi(N)}$ such that $e_0x_0 + y_0 = 0 \bmod \phi(N)$ and $e_1x_1 + y_1 = 0 \bmod \phi(N)$. Assume for contradiction that $e_0 = e_1$. This implies

$$\frac{y_0}{x_0} = \frac{y_1}{x_1} \bmod \phi(N).$$

Note that the fractions are well-defined since $\gcd(x_0, \phi(N)) = 1$ and $\gcd(x_1, \phi(N)) = 1$ by Definition 9.

Equivalently we can write

$$y_0x_1 = y_1x_0 \bmod \phi(N). \tag{7}$$

But $x_0, x_1 \le f$ and $y_0, y_1 \le g$. This implies that both products in the identity above are smaller than $fg < \frac{\phi(N)}{f} \le \frac{\phi(N)}{2}$ in absolute value. Thus, the identity even holds over the integers and not just modulo $\phi(N)$.

By Definition 9, all the tuples $(x, y) \in T(k)$ satisfy the relations $y = k\phi(N) \bmod x$ and $\gcd(x, \phi(N)) = 1$. This implies

$$\gcd(x, y) = \gcd(x, k\phi(N)) = 1.$$

Thus, we have $\gcd(x_0, y_0) = 1$ as well as $\gcd(x_1, y_1) = 1$. We conclude that $x_0 = x_1$ and $y_0 = y_1$ in equation 7, which is a contradiction. Therefore $e_0 \neq e_1$ and the claim follows. $\square$

It remains to derive a lower bound for $|T|$. Our goal is to provide a lower bound for the size of the sets $T(k)$. If the sets $T(k)$ are pairwise distinct then $|T|$ can be bounded by $\sum_{k=\frac{f}{4}+1}^{f} |T(k)|$. The pairwise distinctness is proven in the following lemma.

Lemma 12 *If $k \neq l$ then $T(k) \cap T(l) = \emptyset$.*

Proof: Assume for contradiction that $(x, y) \in T(k), T(l)$ for $k \neq l$. Then

$$y = k\phi(N) \bmod x \quad \text{and} \quad y = l\phi(N) \bmod x.$$

Since $\gcd(x, \phi(N)) = 1$, we can divide both equations by $\phi(N)$. We conclude that $k = l \bmod x$. But $k, l < x$ by Definition 9 and therefore $k = l$ over the integers, contradicting the assumption $k \neq l$. $\square$

In order to provide a lower bound for $|T(k)|$, we fix the parameters N, k and x and sum over all y in $T(k)$. The following technical lemma from the area of analytic number theory gives us a bound for the number of integers y that meet the requirements of Definition 9. Since we want to apply the lemma for different variable settings, we give it a general form and introduce new parameters l, r and u. To understand the connection to the definition of $T(k)$, the reader can substitute the variables l, r by the lower and upper bound $-gx$ and gx, respectively. The variable u can be substituted by $k\phi(N)$ in the following lemma.

Lemma 13 *Let N, $x \in \mathbb{N}$ with $\gcd(x, \phi(N)) = 1$. Let $l, r, u \in \mathbb{Z}$ be arbitrary. The set*

$$\{y \in \mathbb{Z} \mid l < y \le r, y = u \bmod x \text{ and } \gcd(y, \phi(N)) = 1\}$$

contains at least

$$\frac{1}{2\log\log(\phi(N))} \frac{r-l}{x} - \mathcal{O}(N^{\epsilon})$$

elements, where $\epsilon > 0$ is arbitrary small for suitably large N.

Proof: To prove Lemma 13 we need the Moebius μ-function. For $m = p_1 p_2 \cdots p_k \in \mathbb{N}$, $p_1, \ldots, p_k$ prime, it is defined as

1. $\mu(1) = 1$
2. $\mu(m) = (-1)^k$ if all the primes $p_1, \ldots, p_k$ are different.
3. $\mu(m) = 0$ otherwise

Let $y_0 \in \mathbb{Z}_x$ be the unique integer that satisfies $y_0 = u \bmod x$.

Then y, $l < y \leq r$ satisfies $y = u \bmod x$ iff y is of the form $y_0 + tx$ with $\frac{l-y_0}{x} < t \leq \frac{r-y_0}{x}$. A divisor d of $\phi(N)$ divides $y_0 + tx$ iff $t = -\frac{y_0}{x} \bmod d$. Note that the inverse of x modulo d exists since $x \in \mathbb{Z}^*_{\phi(N)}$. In the interval $(\frac{l-y_0}{x}, \frac{r-y_0}{x}]$ there are at least $\lfloor \frac{r-l}{dx} \rfloor$ numbers of this form. By the inclusion-exclusion principle we conclude that the number we are looking for is at least

$$\sum_{d|\phi(N)} \mu(d) \lfloor \frac{r-l}{dx} \rfloor = \sum_{d|\phi(N)} \mu(d) \frac{r-l}{dx} - \sum_{d|\phi(N)} \mu(d) \frac{r - l \bmod dx}{dx}$$

$$\geq \frac{r-l}{x} \sum_{d|\phi(N)} \frac{\mu(d)}{d} - \sum_{d|\phi(N)} |\mu(d)|$$

Since $\displaystyle\sum_{d|\phi(N)} \frac{\mu(d)}{d} = \frac{\phi(\phi(N))}{\phi(N)}$ and $\displaystyle\frac{\phi(\phi(N))}{\phi(N)} \geq \frac{1}{2 \log\log(\phi(N))}$ for N large enough, we get

$$\sum_{d|\phi(N)} \mu(d) \lfloor \frac{r-l}{dx} \rfloor \geq \frac{1}{2 \log\log(\phi(N))} \frac{r-l}{x} - \sum_{d|\phi(N)} |\mu(d)|.$$

Finally we use the fact that $\displaystyle\sum_{d|\phi(N)} |\mu(d)| = \mathcal{O}(\phi^\epsilon(N)) = \mathcal{O}(N^\epsilon)$ for all $\epsilon > 0$ (see [1]). $\square$

If we set $x = 1$, we obtain

Corollary 14 *Let $N \in \mathbb{N}$ and $l, r \in \mathbb{Z}$. The number of integers y with $l < y \leq r$ and $\gcd(y, \phi(N)) = 1$ is at least*

$$\frac{r-l}{2 \log\log(\phi(N))} - \mathcal{O}(N^\epsilon),$$

where $\epsilon > 0$ is arbitrary small for suitably large N.

We are now able to prove a lower bound for $|T| = \sum_{k=\frac{f}{4}+1}^{f} |T(k)|$.

Lemma 15 *Let g, f be as defined in Lemma 6. Then*

$$|T| \geq \frac{f^2 g}{8 \log\log^2(N^2)} - \mathcal{O}(f^2 N^\epsilon),$$

where $\epsilon > 0$ is arbitrary small for suitably large N.

Proof: From Lemma 13 we conclude that for fixed N, k and x the number of $y \in \mathbb{Z}, |y| \leq gx$ such that $(x, y) \in T(k)$ is at least

$$\frac{g}{\log\log(N)} - \mathcal{O}(N^\epsilon).$$

Hence

$$\sum_{k=\frac{f}{4}+1}^{f} |T(k)| \geq \sum_{k=\frac{f}{4}+1}^{f} \sum_{\substack{x=k+1 \\ \gcd(x,k\phi(N))=1}}^{f} \left(\frac{g}{\log\log(N)} - \mathcal{O}(N^\epsilon) \right)$$

$$\geq \left(\frac{g}{\log\log(N)} \sum_{k=\frac{f}{4}+1}^{f} \sum_{\substack{x=k+1 \\ \gcd(x,k\phi(N))=1}}^{f} 1 \right) - \mathcal{O}(f^2(N)N^\epsilon).$$

Applying Corollary 14 shows that for $\epsilon > 0$ arbitrary and N large enough

$$\sum_{\substack{x=k+1 \\ \gcd(x,k\phi(N))=1}}^{f} 1 \geq \frac{f-k}{2\log\log(k\phi(N))} - \mathcal{O}(N^\epsilon).$$

Hence

$$\sum_{k=\frac{f}{4}+1}^{f} \sum_{\substack{x=k+1 \\ \gcd(x,k\phi(N))=1}}^{f} 1 \geq \left(\sum_{k=\frac{f}{4}+1}^{f} \frac{f-k}{2\log\log(kN)} \right) - \mathcal{O}(fN^\epsilon)$$

$$\geq \left(\frac{1}{2\log\log(N^2)} \sum_{k=0}^{\frac{3}{4}f-1} k \right) - \mathcal{O}(fN^\epsilon)$$

$$\geq \tfrac{f^2}{8\log\log(N^2)} - \mathcal{O}(fN^\epsilon).$$

Since $g \leq f$, the lemma follows. ◻